(19) Korean Intellectual Property Office (KR)
(12) Patent Laid-open Publication (A)

(51) Int. Cl.[7]
G06K 19/07

(11) Publication No.: 10-2003-0049387
(43) Publication Date June 25, 2003

(21) Application No: 10-2001-0079581
(22) Filing Date: December 14, 2001

(71) Applicant: NCBIZ CO LTD
Ari B/D. 5F, 162-24 Samsung-dong, Gangnam-gu, Seoul, Korea
Kim, Sung-Woo
Taeyoung Apt. 307-901, Areumvillage, Imae-dong, Bundang-gu, Seongnam City, Gyeonggi-do, Korea
Seo, Won-Il
Mokdong Apt. 219-502, 902 Mok-dong, Yangcheon-gu, Seoul, Korea

(72) Inventor Kim, Sung-Woo
Taeyoung Apt. 307-901, Areumvillage, Imae-dong, Bundang-gu, Seongnam City, Gyeonggi-do, Korea
Seo, Won-Il
Mokdong Apt. 219-502, 902 Mok-dong, Yangcheon-gu, Seoul, Korea

(74) Agent: Kim, Jun-Hyo

Request for Examination: Yes

(54) Title of Invention: EXTENDED SMART CARD SYSTEM AND METHOD FOR CONTROLLING THE SAME

Abstract:

The present invention relates to an extended smart card system and method for controlling the same. The extended smart card system includes a smart card that stores card data including an ID and password of a user, a predetermined applet, and the like; a card reader that reads the card data of the smart card when the smart card is inserted into the card reader; a host PC that is electrically connected to the card reader to store the card data read by the card reader in a certain memory site and to transmit the card data to an outside via a network connected to the outside; and a server that receives the card data transmitted from the host PC and transmits an allowance signal to the host PC via network while allocating a virtual storage of the smart card in the server in response to a positive determination result after determining whether the smart card has an access authority.

Representative Drawing

Fig. 1

Specification

Brief Explanation of Drawings

Fig. 1 is a configuration view of an extended smart card system according to the present invention.

Fig. 2 is a view illustrating a hardware connection configuration among a smart card, a card reader, and a host PC.

Fig. 3 is an extended conceptual view of the smart card according to the present invention.

Fig. 4 is a flow chart of a method for recognizing a smart card according to the present invention as a general drive.

Fig. 5 is a conceptual view of a protocol for recognizing a smart card according to the present invention as a virtual storage.

Fig. 6 is a conceptual view illustrating communication between a server and an application in a host PC according to the present invention.

Fig. 7 is a conceptual view illustrating communication between the smart card and the application in the host PC according to the present invention.

Fig. 8 is a conceptual view of access authority of the smart card to a server's storage.

Description of Reference Numerals for the Drawings

10: smart card 12: card reader 14: host PC 16: network 18: server

Detailed Description of the Invention

Objective of the Invention

Technical Problem to be solved by the Invention

It is an object of the present invention to provide a system that enables a smart cart carried by a user to be used as a portable media solution such as a diskette or CD-ROM for improved convenience. It is another object of the present invention to provide a smart card capable of acting as a mass storage device to provide application programs or data such as virus vaccines.

It is a further object of the present invention to provide a system that can supply a general-application library updated by a card issuer or an application supplier for users of cards thereof and permit the users to use the general-application library.

Constitution and Operation of the Invention

The extended smart card system will be described with reference to Fig. 1.

The extended smart card system comprises a smart card (10), a card reader (12), a host PC (14), and a server (18) connected to the host PC (14) via a network (16).

The smart card (10) stores an ID and password of a smart card user, and applets relating to data and application programs stored in a storage (20) of the server (16).

Here, the term "applet" refers not to a proper noun used for a specific platform, but to an application program in a typical card.

The card reader (12) serves as an information path, though which predetermined data of the smart card, such as the ID, password, and applets, are transmitted to the host PC (14) electrically connected to the card reader (12), or vice versa, when the smart card (10) is inserted into the card reader (12).

The host PC (14) recognizes the smart card (10) as an extended drive, which is one form of storage media, and employs the smart card (10) as a mass storage site. When copying data to the smart card (10), only the applets are generated therein, and the data to be stored is stored not in the smart card (10) but in the storage (20) allocated for the smart card (10) in the server (18), which is connected to the host PC (14) via the network (16). The server (18) has the storage (20) allocated for storing the data and applications for a user of the smart card (10) such that, when the data and applications of the smart card (10) are executed, the data of the server (18) is transmitted to, received from, or executed by the host PC (14).

Configuration of the smart card (10), the card reader (12) and the host PC (14) will hereinafter be described in more detail with reference to Fig. 2.

The smart card (10) comprises a CPU (22) for processing input or output data, a

RAM (24) for temporarily storing data when undergoing data processing, a ROM (26) for storing system programs for operating the card, and an EEPROM (28) for storing predetermined information relating to the applets, and the ID and password of the smart card user. The EEPROM (28) is a non-volatile memory which prevents information stored therein from being erased when power is disconnected and which enables reading and writing of predetermined information when power is supplied thereto. When the smart card (10) is inserted into a socket (30) of the card reader (12), data transmission and reception occur between the smart card (10) and a smart card controller (38), which is connected to a connector 2 (36) of the host PC, via a cable (34) connected between the host PC (14) and a connector 1 (32) electrically connected to the socket (30) in the card reader (12). When the host PC receives the data through the smart card controller (38), a main processor (40) of the host PC processes the data.

One example of using such a smart card as an extended storage will be described hereinafter.

Referring to Fig. 3, an Extended Smart Card Portal Solution (hereinafter, XSCP) (100) enables extension of a virtual EEPROM for the smart card (10). Personal data or general applications for a PC can be stored in a Virtual Storage for XSCP (hereinafter, VSX) (102), and respective applets (104) can store data thereof in the VSX (102).

The VSX (102) is provided with required authority through a network, and a virtual storage in the smart card (10) is actually a section of a server storage.

The VSX (102) makes a user believe that he/she has stored data in the smart card (10) when retrieving a file, but the smart card (10) is actually connected to the server storage via the network.

In other words, since the VSX (102) is recognized as a drive such as a CD-ROM in the file, users believe the server storage to be located as a storage in the smart card (10). The applet (104) of the smart card (10) contains only a small amount of information, such as an ID, password, and the like, as data used for a access control. As described above, if the personal computer (PC) is connected to the network, the users can conveniently employ the smart card (10) as a mass diskette or a readable/recordable CD-ROM. Thus, it is desirable to extend and use the XSCP (100)

to act as a sole portal site in the smart card. The XSCP (100) provides the applets (104) of the smart card (10) and a pair of host PC applications, with which many applets (104) and host PC applications present as pairs can be easily distributed and the users can install the applets/host PC applications merely by clicking an icon in the VSX (102). Additionally, with this configuration, getting updated general-PC application programs and useful data, such as stock information, e-books, movies, etc., is possible.

A method for recognizing the smart card as a general drive will be described with reference to Figs. 3 to 6.

Since the smart card (10) originally acts as a small computer system, the XSCP (100) is designed as an extended storage and enables communication with the storage (20) of the server (18) by means of a file browser, which can cause a user to believe it to be a storage device within the smart card (10). The applets (104) of the smart card (10) include a small amount of data, i.e., personal ID, password, and access authority for files and directories.

When the smart card (10) is inserted into the card reader (200), a specific application (300) of the host PC (14) is executed (202) to read card data or applets (104) from the smart card (10) (204).

Thus, the application (300) of the host PC (14) reads the data from the smart card (10) (204) and transmits the data to the server (18) through a network (206). The server determines whether ID, password, and access authority are identified as complying with those stored in the server (208) and transmits (i.e., replies the determination result to the application (appearing as a drive symbol in a file browser and mapped in the server storage) of the host PC (14) (210)).

If the above condition is satisfied, the host PC recognizes the smart card (10) as a card drive, which is one form of storage media, and permits it to be used (212).

When a user copies certain files to this smart card (10) acting as the card drive, the host PC application (300) transmits the data to the server (18) and completes the transmission (displaying file symbols on the file browser as in general file copying from one folder to another).

Preferably, the respective files transmitted to the server are checked in real time or later by antivirus software in order to protect the files from viral infection.

However, since this can cause delays in execution time or transmission time, it is desirable to check large files simultaneously later as a group while allowing to check important small files in real time.

Fig. 7 is a conceptual view of access authority of the smart card to a server's storage.

A user (400) stores data in a Storage for Personal Data (hereinafter, SPD) (402), which is a folder of the user in the VSX (102). Since the user (400) has authority to read/write/execute data in the folder, the user (400) stores and erases the data (including application programs) while reading and executing other data and files. This section will be divided between the user (400) and other users, and the user (400) must be prevented from accessing data of the other users. Hence, personal activity and materials of the user (400) must be completely concealed. That is, all access authorities to respective folders or directories of users (400, 401) in the VSX (102) are regularly authorized by the users thereof.

Although the XSCP (100) has begun as a virtually extended storage, one of the most important functions thereof is in distributing and sharing general data and applications (hereinafter, GDA) (404) such as contents so that the XSCP (100) acts as Internet portal site. Although it appears to be a folder or a directory, users only have authority to read and execute the folder or directory. Only an XSCP manager (408) has authority to read or update the folder or directory. With this configuration, avoiding the user from deleting data is possible.

Certain data or applications can be configured to allow only a particular user access while appearing invisible to general users. One major feature of smart card technology is the support for multi-application environments, which enables many card applets to be installed in the card. In this case, card issuers must provide the Smart Card Management Systems (SCMS) for distributing the applets and key management. This system is called the Morgue of Applets (hereinafter, MOA) (406). A folder or directory of these applets is not deleted or updated by the users (400, 401) and provides the authority only to the XSCP manager (408). Further, since it is necessary to provide

an application for installation, applet installation must be processed by install tools having predetermined keys. The keys are provided to card issuers or application providers, and different install tools are provided for different card platforms, for example, Visa Open Platform (VOP), the Platform announced by MasterCard (MULTOS), and Windows for smart card. Like the general applications, these tools can be supplied by the XSCP and installed in a user's PC so that the user can install card applets of VSX into his or her card with a single mouse click.

An access Control Privilege (hereinafter, ACP) is one of the most important techniques for the XSCP and allows all of the users (400, 401) to have their respective storage devices including all privileges such as reading/writing/executing/updating allowances when using the ACP. A certain section must be configured to be visible only to particular users, and a certain section must be configured to allow all users (400, 401) only to read that section while allowing the XSCP manager (408) to have all authorities. On the other hand, binary information used in a computer can be freely copied by a user, and copied binary information is the same as original binary information. Thus, there is no difference between the copied binary information and the original binary information.

Accordingly, the present invention enables operation only with a certain physical key, the program of which is copy-protected.

As the physical key, various means can be used. Code-based diskettes, hardware units inserted into a printer port, fingerprint or sound recognition devices, and original CDs can act as the physical key. Such a physical key is copy-protected by integrating a specific code thereto, called a guard module which serves to prevent execution of software if a certain particular initialization is not performed.

The guard module searches the physical key and allows initialization required for program execution to be carried out when the physical key exists therein.

In other words, copy protection is a change of an original code to be operated by a certain external action, and the guard module serves as the physical key or provides required action when recognizing the physical key.

Effects of the Invention

As can be appreciated from the above description, the present invention provides an advantageous effect in that a smart card can be used as a mass storage device irrespective of the storage capacity of an EEPROM having a limited size. Further, the smart card provides a storage device only for a user, thereby enabling the user to use the smart card in any environment where the smart card system is constituted.

Additionally, the present invention provides various access authorities to data and applications stored in a storage of a server, thereby enabling efficient management of the server by a server manager.

(57) WHAT IS CLAIMED IS:

1. An extended smart card system, comprising:

a smart card which stores card data including an ID and password of a user, a predetermined applet, and the like;

a card reader which reads the card data of the smart card when the smart card is inserted into the card reader;

a host PC which is electrically connected to the card reader to store the card data read from the smart card in a certain memory site and to transmit the card data to the outside via a wire/wireless network connected to the outside; and

a server which receives the card data transmitted from the host PC and transmits an allowance signal to the host PC via the wire/wireless network while allocating a virtual storage of the smart card in the server in response to a positive determination result after determining whether the smart card has an access authority.

7. The extended smart card system according to claim 1, wherein the host PC is a PDA.

14. A method for controlling an extended smart card system, comprising the steps of:

(a) inserting a smart card into a card reader by a user;

(b) executing a predetermined application in a host PC;

(c) reading card data of the card reader;

(d) transmitting the card data read at step (c) to a server;

(e) identifying the card data in the server;

(f) transmitting a result signal generated at step (e) to the application of the host PC; and

(g) allowing the user to recognize and use the smart card as a general drive of the host PC in response to confirmation data included in the result signal transmitted at step (e).